Enterprise Risk and Opportunities Management (EROM) Minimum Standards

Issue Date: October 14, 2010
Revised Date: September 12, 2016

Authority

The Crown Corporations Act, 1993
CIC Board Minute #138/2010

Applicability

This policy is applicable to CIC and its subsidiary Crown corporations.

Purpose

This policy establishes minimum Enterprise Risk and Opportunities Management (EROM) standards to be complied with, or exceeded, by those Crowns that submit Performance Management documents to the CIC Board of Directors.

The EROM minimum standards provide the following benefits:

- Establish a sector-wide framework to achieve consistency in EROM application between Crowns;
- Contribute value to Crown sector governance, decision making, and resource allocation processes through demonstration of alignment of key Crown risks and opportunities with performance management plans;
- Provide EROM reporting to CIC to enable a better understanding of subsidiary risk and opportunity profiles;
- Meet or exceed corporate governance best practices and public sector accountability and transparency requirements; and
- Contribute to enhancing and maintaining public confidence in Crown EROM functions.

Policy

Crowns must comply with, or exceed, the minimum standards for EROM outlined in Appendix A.

Administrative Information

Contact: Corporate Controller, Finance & Administration Division, 787-7264.

Reviewed: September 12, 2016

Appendix A

Enterprise Risk and Opportunities Management (EROM) Minimum Standards

Introduction

Background

This document sets out CIC's minimum standards for Crown sector EROM. Applicable CIC subsidiary Crown corporations (Crowns) should have EROM policies and frameworks in place that are materially consistent with these minimum standards.

Organization of this Document

Crowns have flexibility to address CIC's minimum standards for EROM. Crowns are expected to maintain an EROM process that meets best practice in corporate governance while supporting effective decision making and resource allocation processes.

This document presents minimum standards with respect to EROM but is not intended to address all possibilities for policy and framework elements or options.

The minimum standards in this document are organized categorically. However, Crowns are not required to organize EROM in the same manner, provided that overall compliance with the minimum standards can be demonstrated.

Certain EROM elements included in this document are considered leading practice that Crowns are encouraged to follow, but are not mandatory minimum standards. For clarity, minimum standards that Crowns are required to follow are identified with the words "mandatory", "shall", "must", and "will". Words such as "encouraged to" and "consider" indicate leading practices that are suggested but not required by the minimum standards.

GLOSSARY

Term	Definition[1]
Enterprise-wide Risks and Opportunities	Risks and opportunities may occur in defined categories such as: Financial, Mandate, Legal, Compliance and Reporting, Operational, and Reputational.
Critical Success Factors (CSFs)	A limited number of prerequisites and areas of dependency for a strategy or process to be successful. CSFs may be inputs, parallel or supporting activities, or aspects of a business's philosophy or infrastructure necessary to ensure that the strategy or process objectives are met.
Enterprise Risk and Opportunities Management (EROM)	EROM is an integrated enterprise-wide risk and opportunities process established over time which links the management of strategic objectives to risk and opportunities in order to improve corporate performance. It creates a formal process for managing the myriad of risks and opportunities an organization faces. EROM is not the same as risk assessment but the assessment of risk is an integral part of an EROM process.
Inherent Risk	The possibility that risks will prevent an organization from achieving its objectives before the consideration of processes and controls in place to manage or mitigate the risks.
Key Performance Indicators (KPIs)	Key performance indicators (KPIs) are quantitative measurements, both financial and non-financial, of a process's ability to meet objectives and performance. KPIs are usually analyzed through trend analysis within a company or through benchmarking against a peer of the company or its industry.
Magnitude of Impact (sometimes referred to as consequence)	Significance of a particular risk to the entity. The significance of a particular risk can range from insignificant to catastrophic. Magnitude of impact is determined with respect to an organization's risk appetite, risk capacity, and organizational objectives.
Mitigate	To lessen or minimize the adverse impact of a risk through specific management processes or internal control activities.
Likelihood of Occurrence	Probability that a particular risk will occur. These probabilities range from rare to almost certain and are evaluated against an organization's set time period (the organization's strategic planning horizon).
Optimize	To balance potential risks versus potential opportunities within the organization's stated willingness or appetite and capacity to accept risk. This may require an organization to increase or decrease the amount of risk relative to the potential opportunity.
Residual Risk	Risk after considering the effectiveness of management's risk responses (i.e., processes and controls in place to manage or mitigate the risks).
Risk	Internal or external event, activity or situation that impacts an organization's ability to achieve goals.
Risk Appetite	Level of risk an organization is prepared to accept to achieve its goals and objectives (i.e., the level of tolerance for risk in an organization).
Risk Assessment	A risk assessment process allows organizations to consider the extent to which potential events may have an impact on the achievement of organizational objectives. Organizations typically need to identify, assess and evaluate risks and controls to construct an appropriate risk portfolio.
Risk and Opportunities Identification	The process of identifying and understanding potential risks and opportunities.
Risk and Opportunities Management	The process of identifying, evaluating, selecting and implementing an action plan to avoid or mitigate threats and to leverage and maximize, where possible, risk opportunity.
Risk and Opportunities Monitoring	The process of reviewing and evaluating the effectiveness of the action plan implemented through the EROM process and identifying opportunities to minimize future reoccurrence of similar risk.
Risk Opportunity	The return which may be realized if risk is assumed but managed in a manner that maximizes its potential benefit.

[1] It is acknowledged that these terms may be defined differently by various sources. These definitions are presented for the purposes of interpreting this document, and are not required to be utilized by Crowns.

EROM Authority and Governance

EROM Governance

EROM is the responsibility of all Crown stakeholders and therefore must ultimately be embedded into everyday activities of the Crown. It must be considered as part of every decision that is made, every objective that is set, and every process that is designed.

With respect to EROM governance, all Crowns are encouraged to design and implement a structure (i.e. clearly defined roles, accountabilities and responsibilities) that:

- Identifies and evaluates significant risks and opportunities at each level of the enterprise;
- Documents and manages the response to key risks and opportunities;
- Embeds accountability for EROM, thereby enhancing performance management and monitoring;
- Facilitates appropriate risk/opportunity/reward decisions at all levels of management;
- Communicates the risks and opportunities, and management's responses and priorities to all relevant staff; and
- Demonstrates the effectiveness of risk mitigation processes.

Minimum standards for EROM governance include:

- EROM must be "owned" by a member of Executive Management who is accountable for the execution of the EROM policy and framework. However, the "owner" is not required to personally execute the myriad of EROM activities. The "owner" can designate an individual (e.g. an enterprise risk and opportunities manager) or group (e.g. internal audit) to facilitate certain of EROM activities under the "owners" direction.
- The Board of Directors of each Crown must take ultimate responsibility for EROM. The Board may delegate certain EROM activities to a Board committee for efficiency purposes, but must remain ultimately responsible for EROM. This responsibility must be demonstrated via Board review and acceptance of at least the following items:
    - The Crown's EROM policy and framework;
    - Management's risk appetite and tolerance levels;
    - Management's summary risk and opportunities register as well as the assessment results for the Crown's top corporate-wide risks and opportunities;
    - Management's list of processes and controls that are relied upon to mitigate the Crown's top risks;
    - Management's identification of gaps where identified risks are either over-mitigated or under-mitigated. This includes identification of opportunities and strategies to either close gaps where residual risk is higher than assessed risk appetite or to reallocate resources from areas where residual risk is lower than assessed risk appetite;
    - Management's identification of innovations/opportunities/upside leveraging related to risks identified;
    - Action plans to address risk mitigations and opportunities identified as high priority by management; and
    - Regular reports from the Executive Management "owner".

EROM Policy

In order to provide legitimacy and formality to the process, Crowns must include the EROM governance structure in a duly approved Corporate policy, including a timeframe for regular review and approval of the policy.

In addition, Crowns are encouraged to include formal recurring activities (e.g. monitoring activities and reporting requirements) and related timeframes in the EROM policy.

The EROM policy, and any future updates to the policy, must be formally approved by the Crown's Executive Management and Board of Directors.

EROM Framework

Crowns shall include detailed elements of EROM processes and practices (e.g. accepted definitions, risk categories, risk appetite, approach to risk and opportunities management, assessment criteria, mitigation assessment criteria, tools and templates, monitoring and reporting practices, etc.) into a formal EROM framework. This framework contains significantly more detail about recurring EROM processes and practices than the EROM policy.

The Crown EROM framework, and any future updates to the framework, must be formally approved by the Crown's Executive Management and Board of Directors.

Approach to EROM

Use of Widely Accepted EROM Frameworks

Crowns shall utilize an established EROM framework (for example COSO framework) as a guide when developing and evolving EROM processes and practices.

Risk and Opportunities Identification

There are several approaches utilized for identifying key risks:

- Top-down approach: focuses on identifying enterprise-wide risks and opportunities that affect an entity's strategic goals and objectives - usually includes direct involvement by senior management and the Board of Directors in the process.
- Bottom-up approach: focuses on identifying key operational and tactical risks and opportunities on a divisional or business unit basis.
- Hybrid approach: focuses on identifying key operational and tactical risks and opportunities on a divisional or business unit basis then integrating results to derive the key enterprise-wide risks and opportunities.

Crowns have the flexibility to choose the risk and opportunity identification approach appropriate to its circumstances. However, each Crown's identification process must ultimately produce an overall register that contains the Crown's top enterprise-wide risks and opportunities.

When identifying top enterprise-wide risks and opportunities, Crowns shall consider:

- Current and future expected risks and opportunities present within its industry;
- Risks and opportunities associated with recent internal changes in the business;
- Risks and opportunities associated with external change; and
- Root causes for the risks and opportunities (i.e. the source of the risk or opportunity, including why, how, and where it originates (either outside the organization or within its processes or activities).

Identification of risks and opportunities occurs on an: (1) on-going basis for existing processes and; (2) ad-hoc basis for new processes or changes to existing processes.

Risk Assessment

A clear assessment of the most significant enterprise-wide risks allows the Crown to focus management effort on those processes and controls required to address those risks.

- Requirement to Perform Risk Assessments

  Crowns must assess at least the top enterprise-wide risks in order to determine those most significant to corporate success. To add rigour and credibility to the results, Crowns must involve Executive Management in the assessment process, and are encouraged to involve the Board of Directors.

- Requirement to Develop and Utilize Risk Assessment Criteria

  In order to assess risks in a consistent and meaningful manner, Crowns must develop and utilize formal risk assessment criteria based upon both the magnitude of impact and likelihood of occurrence. Crowns have the flexibility to select the scale utilized in the assessment (e.g. High/Medium/Low, 3 point numeric, 5 point numeric, etc.).

- Inherent vs. Residual Risk Assessments

  Crowns must perform risk assessments on both an inherent and residual basis in order to achieve maximum value from the process. The difference between the inherent ranking and residual ranking for a risk serves as a tool for management to determine the effectiveness of mitigating processes and controls in managing the related risk exposure.

  Once the relationship between a Crown's key risks and mitigations is better understood, management can begin to identify areas where: i) mitigating processes and controls are being heavily relied upon to manage certain risks; ii) there may be insufficient or ineffective processes and controls in place to manage certain risks; and iii) risks may be over-controlled given the inherent risk profile (i.e. fewer controls may be necessary and resources reallocated to areas facing greater risk).

Additional Information to be Captured and Reported

- Mitigating Processes and Controls

  For the top enterprise-wide risks, Crowns must identify key mitigation processes and controls in place to manage those risks. This should include information about what is actually being done to manage the risk, and should include only those mitigations that are demonstrably managed and clearly related to the risk in question.

  Crowns must also assess the effectiveness of the key mitigations to understand the difference between inherent and residual risk. The mitigation effectiveness assessment should be based upon formal criteria developed by the Crown and may include: testing by management; a self-assessment process; involvement of internal audit; development and monitoring of relevant critical success factors (CSFs) or key performance indicators (KPIs); or another acceptable means of evaluation.

  Crowns are encouraged to include information on mitigating controls and processes directly within the summary risk and opportunity register.

- Identification of Risk and Opportunity Owners

  In order to allocate responsibility for the continuous management of each risk and opportunity, all Crowns are required to designate explicit "owners" for the top enterprise-wide risks and opportunities, including corresponding key mitigating risk controls and processes. Crowns are encouraged to include this information directly within the summary risk and opportunity register.

  Crowns are encouraged to avoid delegating multiple "owners" for individual risks, opportunities and mitigations given the potential to blur primary responsibility and accountability.

- Strategies to Address Key Risks Not Sufficiently Mitigated

  Once desired levels of control effectiveness are determined, any material gaps between existing and desired control effectiveness must result in an action plan to address the gap. Key risks that are not sufficiently mitigated must be disclosed to Executive Management, and formal strategies must be developed to address gaps over an appropriate time period.

  Crowns must document in a risk and opportunities register or a supporting document whether the top enterprise-wide risks are sufficiently managed and any related action plans. Action plans for identified key opportunities must include a formal strategy to capitalize on the opportunity over an appropriate period of time.

  The action plans must be unambiguous and should provide target dates and names of responsible persons.

Timing of Risk Assessments

Unless there is some unavoidable reason that would make doing so impracticable, Crowns shall update the risk and opportunity identification and assessment results at least annually in order to validate or update the prioritized summary risk and opportunities register.

Ongoing Monitoring

Crowns must perform semi-annual, formal, high-level reviews of the summary risk and opportunities register to identify and evaluate new or changed risks, opportunities, or mitigations and report the results to Executive Management and the Board of Directors. Such a monitoring process helps ensure that risks and opportunities are being analyzed to identify patterns and accumulations, and ensure that enterprise-wide responses are effectively planned and implemented where necessary.

Crowns are encouraged to determine if any KPIs can be utilized to monitor risk and opportunity trends on an ongoing basis.

Risk Appetite

Risk appetite is defined as the level of risk an organization is prepared to accept to achieve its goals and objectives (i.e. the level of tolerance for risk in an organization). In other words, at what point does a risk become serious enough for an organization to start committing additional time and effort into its management? For example:

- If a risk is assessed as above an organization's risk tolerance, the typical management strategy is to either implement action plans in order to reduce the impact or likelihood of the risk (i.e. implement additional mitigating processes or controls) or avoid the risk (i.e. exit the underlying business line).

- If a risk is assessed as below an organization's risk tolerance, there is an opportunity for management to discontinue mitigating processes or controls that exist solely to manage this risk and reallocate the resources to more value-added activities.

Overall Risk Tolerance Limits

Crowns are encouraged to discuss risk appetite with Executive Management and the Board of Directors, and consider establishment of risk tolerance limits that assist in determining whether a situation is unacceptable, or requires specific management and monitoring.
Some organizations have attempted to address overall risk tolerance limits by establishing a risk assessment rating above which specific actions are required to be undertaken thereby ensuring that the highest ranked risks are sufficiently managed. For example:

- An organization uses a 5 point scale when ranking the impact and likelihood of its risks, and then multiplies the impact and likelihood results to determine a risk's final ranking (maximum score 25). The organization determines that any risk with a score of 20 or higher must be "owned" by a Vice President, related mitigations must be reviewed by internal audit, and there must be specific reporting to the Executive on a quarterly basis.

Risk-specific Risk Tolerance Limits

Crowns that find it impracticable to establish overall risk tolerance limits are encouraged to establish and monitor specific risk tolerance limits for the highest ranked key risks. To achieve this, some organizations establish and monitor critical success factors (CFSs) or key performance indicators (KPIs) for specific risks to determine how well the risk is being managed. For example:

- To address customer service risk, a target on-time completion of customer projects of 98 per cent is set, with the acceptable level of variation between 97–100 per cent.
  The on-time completion rates are regularly monitored to determine if the risk is being appropriately managed.
- To address risks related to employee turnover and succession, an organization establishes targets of 3 per cent annual voluntary turnover and filling 75 per cent of vacant key positions by individuals identified in the succession plan. It then monitors these KPIs to determine if the risk is being appropriately managed.

Approval of Risk Appetite

Crowns must receive the following approvals in cases where formal risk tolerance limits are established:

- Overall risk tolerance limits that apply to all risks or to certain broad risk categories must be documented in the risk and opportunities framework (which must then be approved by Executive Management and the Board of Directors per section 3.3).
- Risk tolerance limits that apply to specific high-ranked risks must be approved by the designated risk "owners" and Executive Management.

Reporting

Internal Reporting

Crowns are encouraged to develop a process to communicate risk assessment results (e.g. the summary risk and opportunities register, corresponding mitigations, and mitigation owners) throughout the organization, so that all staff understand key enterprise-wide risks and opportunities, and appreciate their role in managing them.

- Mandatory Internal Reporting

  Crowns must adhere to the following minimum reporting standards regarding internal risk and opportunity reporting (Crowns may determine the format of the reporting, as long as the required elements are included):

  Reporting Assessment Results: Upon the completion of the assessment process, Crowns must report at least the following to Executive Management and the Board of Directors:
  - The summary risk and opportunities register;
  - The corresponding key risk mitigation processes or controls;
  - The designated risk and control owners;
  - Management's assessment of the effectiveness of the key risk mitigation processes or controls (if assessments have been performed);
  - Any strategies/action plans that were developed to address key risks that were determined to be insufficiently mitigated or opportunities that will be pursued.

  Status Reporting for Specific EROM Strategies: For any strategies/action plans, the owner must provide status reporting to Executive Management at least quarterly.

  Ongoing Monitoring: Refer to section 5 for reporting requirements related to ongoing risk and opportunity monitoring.

  Situational Ad Hoc Reporting: Formal ad hoc risk reports are required to be submitted to Executive Management and the Board when:
  - New key enterprise-wide risks have materialized between regular assessment and monitoring periods, and material changes to the risk, opportunity or mitigation landscape across the Crown are identified; and
  - Material breakdowns in key mitigation processes or controls are identified.

  Verbal discussion and/or informal reporting of the above situations are not considered sufficient.

External Reporting

All Crowns must adhere to the following reporting standards regarding external reporting:

- Reporting to CIC

  All Crowns must provide CIC with a copy of:
  - EROM reporting packages provided to the Crown Board of Directors (must be provided within one week after the Board meeting where the report was presented); and
  - Any ad hoc reports relating to material breakdowns in key mitigating processes or controls (must be provided immediately after the Executive meeting where the report was presented).

- Reporting in the Annual Report

  Crowns are required to ensure any discussion of EROM within the Management Discussion and Analysis is consistent with annual EROM results.

- Reporting in the Balanced Scorecard

  Crowns must consider if Balanced Scorecard measures related to EROM would be an effective addition to the performance management system.

Integration into the Planning and Decision Making Process

Business Planning Process

Crowns shall ensure that the top enterprise-wide risks and opportunities, corresponding mitigating processes and controls, and related action plans are formally discussed and considered during the development of the corporate business plan, as well as any business unit/divisional business plans.

Budgeting Process

Crowns shall formally integrate EROM results into the budgeting process. The benefits of doing so include:

- Helping to ensure that any requests for additional funding are viewed through an EROM lens (i.e. if there is competition for scarce resources, activities that mitigate key enterprise-wide risks or capitalize on key opportunities would typically get priority).
- Helping to ensure that any requirements to reduce costs are viewed through an EROM lens (i.e. do not eliminate activities that mitigate key enterprise-wide risks without careful consideration).
- Helping to ensure that budget is secured for any strategies that have been developed to address key risks that are not being sufficiently mitigated or opportunities that will be pursued.

Internal Audit Process

Crowns should link EROM with Internal Audit to assist in management's assessment of the effectiveness of risk mitigation processes and controls (which in turn affects the accuracy of residual risk assessments). Crowns shall ensure that:

- Internal Audit is provided with the annual EROM results (e.g. provide a copy of the report presented to Executive Management) for consideration when drafting his or her annual internal audit plan.
- Internal Audit must demonstrate to Executive Management how his or her annual internal audit plan takes into account the EROM results.

Reviewed: June 15, 2015